Practitioner's Docket No. NAI1P089/00.175.01 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Peter T. Dinsmore et al.

Application No.: 09/836,214 Group No.: 2131
Filed: 04/18/2001 Examiner: Christian A. Laforgia
For: SYSTEM AND METHOD FOR REUSABLE EFFICIENT KEY DISTRIBUTION

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION--37 C.F.R. § 41.37)

1. This brief is in furtherance of the Notice of Appeal, filed in this case on November 20, 2006, and in response to the Notice of Panel Decision from Pre-Appeal Brief Review, mailed December 20, 2006.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

other than a small entity	$500.00
Appeal Brief fee due	**$500.00**

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	$500.00
Extension fee (if any)	$0.00
TOTAL FEE DUE	**$500.00**

6. FEE PAYMENT

Authorization is hereby made to charge the amount of $500.00 to Deposit Account No. 50-1351(Order No.NAI1P089).

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351(Order No.NAI1P089).

/KEVINZILKA/

Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:)
)
Dinsmore et al.) Group Art Unit: 2131
)
Application No. 09/836,214) Examiner: Laforgia, Christian A.
)
Filed: April 18, 2001) Date: January 22, 2007
)
For: SYSTEM AND METHOD FOR)
REUSABLE EFFICIENT KEY)
DISTRIBUTION)
)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on November 20, 2006, and in response to the Notice of Panel Decision from Pre-Appeal Brief Review, mailed December 20, 2006.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals, interferences, or related judicial proceedings.

A Related Proceedings Appendix is appended hereto.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are. 1-9, 11-15, 17-21, 28-30, and 38-41

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1-9, 11-15, 17-21, 28-30, and 38-41
3. Claims allowed: None
4. Claims rejected: 1-9, 11-15, 17-21, 28-30, and 38-41
5. Claims cancelled: 10, 16, 22-27, and 31-37

C. CLAIMS ON APPEAL

The claims on appeal are: 1-9, 11-15, 17-21, 28-30, and 38-41

See additional status information in the Appendix of Claims.

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, there are no such amendments after final.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claim 1, as shown in Figures 3A-13, a secret updating method is provided in an environment that includes a plurality of users, where each user possesses secrets that are shared by respective sets of the plurality of users. In use, at least one compromised secret known by at least one evicted user is updated using at least one non-compromised secret that is not known by the at least one evicted user. Additionally, the updating does not use new secret information. See, for example, page 15, paragraph [1062]-page 16, paragraph [1064], page 17, paragraph [1068]; pages 17-18, paragraph [1070]; and page 20, paragraphs [1080]-[1081] et al.

With respect to a summary of Claim 13, as shown in Figures 3A-13, a keying method is provided in an environment that includes a plurality of users, where a first user possesses a set of keys, which includes a first key that enables secure communication among a set of users, and where the set of users includes at least the first user and a second user. In use, an updated first key is determined upon eviction of at least the second user using information that includes the first key and a second key. In addition, the second key enables secure communication among a subgroup of the set of users. Moreover, the subgroup does not include users subject to the eviction. Further, the updated first key is determined using a function having the following properties: (1) knowledge of the updated first key does not give knowledge of the first key or the second key, (2) knowledge of the first key does not give any knowledge of the updated first key, and (3) knowledge of the first key and the updated first key does not give any knowledge of the second key. See, for example, page 15, paragraph [1062]-page 16, paragraph [1064]; page 17, paragraph [1068]; pages 17-18, paragraph [1070]; and page 20, paragraphs [1080]-[1081] et al.

With respect to a summary of Claim 28, as shown in Figures 3A-13, a keying method is provided in an environment having a plurality of users, where each user is capable of storing a set of keys that enable secure communication among sets of the plurality of users. In use, first information is distributed that enables users to update, after eviction of one or more users, a set of compromised keys that are known to the one or more users without receiving new key information. In addition, the update does not include new secret information. See, for example, page 15, paragraph [1062]-page 16, paragraph [1064]; page 17, paragraph [1068]; pages 17-18, paragraph [1070]; and page 20, paragraphs [1080]-[1081] et al.

With respect to a summary of Claim 38, as shown in Figures 3A-13, a secret sharing system is provided. In use, a key server distributes secret information to a plurality of users, where each user is sent secrets that are shared by respective sets of the plurality of users. In addition, the key server is operative to update at least one compromised secret known by at least one evicted user using at least one non-compromised secret that is not known by the at least one evicted user. Further, the update does not include new secret information. See, for example, page 15, paragraph [1062]-page 16, paragraph [1064]; page 17, paragraph [1068]; pages 17-18, paragraph [1070]; and page 20, paragraphs [1080]-[1081] et al.

With respect to a summary of Claim 39, as shown in Figures 3A-13, a computer program product is provided. In use, computer-readable program code causes a computer, in an environment that includes a plurality of users where each user possesses secrets that are shared by respective sets of the users, to update at least one compromised secret known by at least one evicted user using at least one non-compromised secret that is not known by the at least one evicted user. A computer-usable medium is also configured to store the computer-readable program codes. In addition, the update does not include new secret information. See, for example, page 15, paragraph [1062]-page 16, paragraph [1064]; page 17, paragraph [1068]; pages 17-18, paragraph [1070]; and page 20, paragraphs [1080]-[1081] et al.

Of course, the above citations are merely examples of the above claim language and should not be construed as limiting in any manner.

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has rejected Claims 1-6, 8-16, 19-21, and 40 under 35 U.S.C. 102(e) as being anticipated by Gundavelli et al. (U.S. Patent No. 6,941,457).

Issue # 2: The Examiner has rejected Claims 28-30 under 35 U.S.C. 102(e) as being anticipated by Dondeti et al. (U.S. Patent No. 6,240,188).

Issue # 3: The Examiner has rejected Claims 38 and 39 under 35 U.S.C. 102(e) as being anticipated by Kadansky et al. (U.S. Patent No. 6,295,361).

Issue # 4: The Examiner has rejected Claim 7 under 35 U.S.C. 103(a) as being anticipated by Gundavelli et al. (U.S. Patent No. 6,941,457) in view of Takeda et al. (U.S. Patent No. 6,178,244).

Issue # 5: The Examiner has rejected Claims 17, 18, and 41 under 35 U.S.C. 103(a) as being anticipated by Gundavelli et al. (U.S. Patent No. 6,941,457) in view of Dondeti et al. (U.S. Patent No. 6,240,188).

VII ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue # 1:

The Examiner has rejected Claims 1-6, 8-16, 19-21, and 40 under 35 U.S.C. 102(e) as being anticipated by Gundavelli et al. (U.S. Patent No. 6,941,457).

Group #1: Claims 1-6, 8-9, and 11-12

With respect to independent Claim 1, the Examiner has relied on the following excerpts from Gundavelli to make a prior art showing of appellant's claimed technique "wherein said updating does not use new secret information."

> "According to another aspect, **upon determining that a first departing member has left the second multicast group a private multicast group non-zero random integer is selected. A second multicast group exchange key is then generated based on a private multicast group non-zero random integer, a public non-zero integer and a public prime integer.** The second multicast group exchange key is then broadcast to each remaining member of the second multicast group for computing a third secret key that is based on the second multicast group exchange key and the second shared secret key. Through the use of the third shared secret key a third multicast group is established whose members include only remaining members of the second multi-cast group as the third shared secret key provides a second secure channel for communicating between members of the third multicast group over the insecure network." (Col. 5, lines 47-63 – emphasis added)

> "Although the examples provided herein illustrate adding users to a multicast group dynamically, the techniques described are also applicable to multicast groups in which members are deleted dynamically. For example, the multicast group may desire to exclude a member who has left the group from future communications between the remaining members. In certain embodiments, when a member leaves the multicast group, a new shared secret key is generated for communicating between those members that remain in the multicast group. Using the new shared secret key, the members remaining in the multicast group can communicate over a secure channel and the departed member cannot decrypt the communications.
>
> In one embodiment, when a person leaves the group, a new shared secret key is established using the traditional Diffie-Hellman algorithm. The

> remaining members may then use the newly established shared secret key to securely communicate with each other. In addition, the new members may be admitted into the group using the method described above.
>
> For example, referring to FIG. 3E, if Carol 314 leaves the multicast group 328, the remaining members within multicast group 330 may establish a new secret key using the traditional Diffie-Hellman algorithm. In addition, the multicast group 330 may compute a multicast group 330 exchange key for admitting new members into the multicast group 330. For example, upon Carol 314 leaving multicast group 328, multicast group 330 may communicate with each other to compute a new shared secret key k4 using the traditional Diffie-Hellman algorithm. In addition, the multicast group 330 may compute an exchange key K3' as previously explained above, for admitting new members into the multicast group 330. For example, the exchange key K3' may be computed as K3'=(g.sup.k4 mod (n))." (Col. 11, lines 6-39)

Appellant respectfully asserts that the above excerpts cited by the Examiner actually *teach away* from appellant's specific claim language. In particular, Gundavelli discloses that "upon determining that a first departing member has left the second multicast group a private multicast group non-zero random integer is selected." Further, Gundavelli discloses that "[a] second multicast group exchange key is then generated based on a private multicast group non-zero random integer, a public non-zero integer and a public prime integer."

Thus, in Gundavelli when a member has left a group, new secret information is utilized in creating the exchange key, including "a private multicast group non-zero random integer, a public non-zero integer and a public prime integer," as expressly disclosed. Appellant, on the other hand, claims that the "updating does not use new secret information" (emphasis added), as claimed.

In the Office Action mailed 07/24/06, the Examiner has "interpreted secret as key, and new secret information as generating a new key." Further, the Examiner has argued that "Gundavelli states in the cited sections that a new group key is generated using the traditional Diffie-Hellman approach, which is to generate a group key using the members already existing keys…[and that t]herefore, Gundavelli discloses updating a secret without using new secret information."

Appellant respectfully disagrees and points out the steps of the traditional Diffie-Hellman approach, as found in the Gundavelli reference:

> "A known public key exchange method is the Diffie-Hellman algorithm described in U.S. Pat. No. 4,200,770. The Diffie-Hellman method relies on the difficulty associated with calculating discrete logarithms in a finite field. According to this method, two participants, A and B, **each select random large numbers a and b, which are kept secret.** A and B also agree (publicly) upon a base number p and a large prime number q, such that p is primitive mod q. A and B exchange the values of p and q over a non-secure channel or publish them in a database that both can access. Then A and B each privately compute public keys A and B, respectively..." (Col. 3, lines 5-16 - emphasis added)

As emphasized in the above excerpt, the Diffie-Hellman approach requires that the participants "each select random large numbers a and b, which are kept secret" (emphasis added). Furthermore, Gundavelli states that "the remaining members within multicast group 330 may establish a new secret key using the traditional Diffie-Hellman algorithm" (Col. 11, lines 3-35) and that "according to [the Diffie-Hellman] method, each [of the participants] select random large numbers a and b, which are kept secret" (emphasis added). Thus, in Gundavelli, when a member has left a group, new secret information, namely random large numbers, are utilized in creating the new secret key. Appellant, on the other hand, claims that the "updating does not use new secret information" (emphasis added), as claimed. Clearly, utilizing new secret information when a member leaves the group, as in Gundavelli, fails to disclose and even *teaches away* from "not us[ing] new secret information" (emphasis added), as claimed by appellant.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim. This criterion has simply not been met by the prior art reference relied on by the Examiner, as noted above.

Group #2: Claims 13-15, and 19-21

With respect to independent Claim 13, the Examiner has again relied on Col. 5, lines 47-63; and Col. 11, lines 6-39 from Gundavelli (reproduced above) to make a prior art showing of appellant's claimed technique "wherein said determining uses a function having the following properties: (1) knowledge of said updated first key does not give knowledge of said first key or said second key, (2) knowledge of said first key does not give any knowledge of said updated first key, and (3) knowledge of said first key and said updated first key does not give any knowledge of said second key."

Appellant respectfully asserts that simply nowhere in Gundavelli is there any disclosure that "knowledge of said first key and said updated first key does not give any knowledge of said second key," as specifically claimed by appellant. In fact, appellant notes that such excerpts only disclose utilizing random integers to create an updated key (see emphasized excerpt above) and using the traditional Diffie-Hellman algorithm to create a new shared secret key. Clearly, such teachings do not even suggest that "knowledge of said first key and said updated first key does not give any knowledge of said second key," as specifically claimed by appellant.

In the Office Action mailed 07/24/06, the Examiner has argued that "[appellant] claims descriptive material that is the reasoning behind updating the compromised key, [that] it allows for the updating of the group key without compromising any member of the group's key...[and that t]herefore, Gundavelli discloses knowledge of the first key and updated first key does not give any knowledge of said second key, thereby making the keys resistant to collusion attacks."

Appellant respectfully disagrees and asserts that in Gundavelli, a new secret key (i.e. third shared secret key) is generated for a group in which a member has left. The new secret key is generated utilizing an exchange key that is based on integers (i.e. non-zero random integer, public non-zero integer, and public prime integer) and a second shared secret key that was used by the group that included the member that left (see particularly Col. 5 of Gundavelli). Thus, in Gundavelli, knowledge of the new secret key inherently includes knowledge of the second shared key since the members are the same except for the member that left. Therefore, Gundavelli teaches away from appellant's claimed "knowledge of said first key <u>and said updated first key</u> <u>does not give any knowledge of said second key</u>" (emphasis added), as specifically claimed by appellant.

Again, the foregoing anticipation criterion has simply not been met by the above reference, as noted above.

Group #3: Claims 10 and 16

Appellant respectfully asserts that Claims 10 and 16 were cancelled in the Substitute Amendment dated 5/10/2006.

Group #4: Claim 40

With respect to dependent Claim 40, the Examiner has relied on Col. 11, lines 6-39 of the Gundavelli reference (reproduced above) to make a prior art showing of appellant's claimed technique "wherein said non-compromised secret utilized for said updating is known by all users in said plurality of users and is not known by said at least one evicted user."

Appellant respectfully asserts that the excerpt from Gundavelli relied upon by the Examiner merely discloses that "when a member leaves the multicast group, a new shared secret key is generated for communicating between those members that remain in the multicast group" (emphasis added). Further, Gundavelli discloses that "when a person leaves the group, a new shared secret key is established using the traditional Diffie-Hellman algorithm" and "[t]he remaining members may then use the newly established shared secret key to securely communicate with each other" (emphasis added). However, the mere disclosure that when a member leaves a group, a new shared secret key is generated for the remaining members to securely communicate, as in Gundavelli, simply fails to even suggest the use of a non-compromised secret, much less a "non-compromised secret [that is] utilized for said updating is known by all users in said plurality of users and is not known by said at least one evicted user" (emphasis added), as claimed.

Again, the foregoing anticipation criterion has simply not been met by the above reference, as noted above.

Issue # 2:

The Examiner has rejected Claims 28-30 under 35 U.S.C. 102(e) as being anticipated by Dondeti et al. (U.S. Patent No. 6,240,188).

Group #1: Claims 28-30

With respect to independent Claim 28, the Examiner has relied on the following excerpt from the Dondeti reference to make a prior art showing of appellant's claimed technique "wherein said update does not include new secret information."

> "B. Leave Protocol
>
> **When a member 22 leaves, its neighbor initiates the rekeying process.** If the neighbor is the departing member's sibling, it assumes its parent's position in the key distribution tree. Otherwise it notifies the descendants of the departing member's sibling to change their IDs. In either case, the neighbor changes its secret key 28 and initiates the rekeying process. **It sends the new keys to the members of its key association group and they are responsible for propagating the new keys to the appropriate members in their subgroups.** In the rest of this section, we describe the ID update process followed by the rekeying process.
>
> X is the departing node and Y (=Neighbor(X)) is its neighbor, step 112. If Y has the same ID length as X, Y right shifts its ID by one bit position to get its new ID. If Y's ID is longer than that of X, X's sibling and its descendants change their IDs as follows. Notice that each descendant Z of X's sibling shares a key with X. If Z=b.sub.h b.sub.h-1 . . . b.sub.i+1 b.sub.i b.sub.i-1 . . . b.sub.2 b.sub.1, then Z's ID after the departure would be b.sub.h b.sub.h-1 . . . b.sub.i+1 b.sub.i-1. . . b.sub.2 b.sub.1, where i is the difference in the length of Z's and X's IDs plus one, step 114. In both cases, Y generates the new secret key and initiates the rekeying, step 116. In FIG. 4, if E leaves, F gets the ID 10 and generates a new secret key; if G leaves, H and I get the IDs 110, 111 respectively and H generates the new secret key.
> Referring to FIGS. 1 and 4, C 50 leaves the multicast group. J 56 notices the departure and changes its ID from 0101 to 010, and generates a new secret key 28 for itself. Consequently, internal node keys on J's path to the root 54 change and J 56 is responsible for initiating key exchanges with its counterparts, 011(D), 000(A) and 110(G) as defined earlier in this section. J 56 sends the blinded key k'.sub.010 to D 48. Both J 56 and D 48 can now compute k.sub.01. J 56 then sends k'.sub.01, to A 52, which is responsible for sharing it with all members who have k.sub.00. Finally, J 56 sends k'.sub.0 to G 44, which in turn sends k'.sub.0 to all the members that have k.sub.1. Notice that J 56 does not need any keys in return from D 48, A 52, or G 44, step 118; It already has the blinded keys it needs to compute the root key, step 120. While the departing member C 50 knows all those blinded keys as well, it does not know any unblinded keys it needs and thus cannot compute or acquire the root key. A departure results in O(log n) multicast messages, each message carrying one encrypted secret key. In the following, we provide a generalization of the rekeying process after a member departs from the group." (Col. 8, line 43 - Col. 9, line 19 - emphasis added)

Appellant respectfully asserts that the excerpt from Dondeti relied upon by the Examiner merely discloses that "[w]hen a member 22 leaves, its neighbor initiates the rekeying process" and that "[i]t sends the new keys to the members of its key association group and they are responsible for propagating the new keys to the appropriate members in their subgroups" (emphasis added). However, the mere disclosure that new keys are sent to the members of the group when a member leaves, as in Dondeti, simply fails to specifically suggest a claimed technique "wherein said update does not include new secret information" (emphasis added), as claimed by appellant.

Again, the foregoing anticipation criterion has simply not been met by the above reference, as noted above.

Issue # 3:

The Examiner has rejected Claims 38 and 39 under 35 U.S.C. 102(e) as being anticipated by Kadansky et al. (U.S. Patent No. 6,295,361).

Group #1: Claims 38 and 39

With respect to independent Claims 38 and 39, the Examiner has relied on Col. 1, line 66-Col. 2, line 61 in Kadansky to make a prior art showing of appellant's claimed technique "wherein said update does not include new secret information."

Appellant respectfully asserts that such excerpt, along with the entire Kadansky reference, only relates to a method of distributing a new group key, but does not even suggest how such new group key is created. Thus, simply nowhere in Kadansky is there any teaching of an "update [that] does not include new secret information" where such update is used for updating "at least one compromised secret known by at least one evicted user" (emphasis added), in the context claimed by appellant.

Again, the foregoing anticipation criterion has simply not been met by the above reference, as noted above.

Issue # 4:

The Examiner has rejected Claim 7 under 35 U.S.C. 103(a) as being anticipated by Gundavelli et al. (U.S. Patent No. 6,941,457) in view of Takeda et al. (U.S. Patent No. 6,178,244).

Group #1: Claim 7

With respect to dependent Claim 7, the Examiner has relied on the following excerpt in Takeda to make a prior art showing of appellant's claimed technique "wherein said updating occurs on a periodic basis."

> "In the above key distributing procedure, **the session key is updated right after receiving the session key.** However, the session key can be updated when the communication is interrupted. Further, the session key can be updated when a predetermined time period has passed after receiving the session key."(Col. 12, lines 38-43 - emphasis added)

Appellant respectfully asserts that such excerpt relied on by the Examiner does not teach updating at least one compromised secret "on a periodic basis," in the context claimed by appellant. Instead, Takeda only discloses updating a session key in response to certain circumstances, namely "right after receiving the session key," "when the communication is interrupted," and "when a predetermined time period has passed after receiving the session key." Clearly, such circumstances do <u>not</u> meet any sort of <u>periodic basis</u>, in the context as claimed by appellant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*,947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Issue # 5:

The Examiner has rejected Claims 17, 18, and 41 under 35 U.S.C. 103(a) as being anticipated by Gundavelli et al. (U.S. Patent No. 6,941,457) in view of Dondeti et al. (U.S. Patent No. 6,240,188).

Group #1: Claims 17 and 18

Appellant respectfully asserts that such claims are not met by the prior art for the reasons argued with respect to Issue #1, Group #2.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #2: Claim 41

Appellant respectfully asserts that such claims are not met by the prior art for the reasons argued with respect to Issue #1, Group #4.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

VIII CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) In an environment that includes a plurality of users , wherein each user possesses secrets that are shared by respective sets of said plurality of users, a secret updating method, comprising:

(a) updating at least one compromised secret known by at least one evicted user using at least one non-compromised secret that is not known by said at least one evicted user;

wherein said updating does not use new secret information.

2. (Original) The method of claim 1, wherein said updating comprises updating a plurality of compromised secrets.

3. (Original) The method of claim 1, wherein said updating comprises updating all compromised secrets.

4. (Original) The method of claim 1, wherein said updating comprises updating at least one compromised secret known by one evicted user.

5. (Original) The method of claim 4, wherein said updating occurs upon an eviction event.

6. (Original) The method of claim 1, wherein said updating comprises updating at least one compromised secret known by a plurality of evicted users.

7. (Original) The method of claim 6, wherein said updating occurs on a periodic basis.

8. (Original) The method of claim 1, wherein said updating comprises updating a compromised secret using one non-compromised secret.

9. (Original) The method of claim 1, wherein said updating comprises updating a compromised secret known by a set of users using a non-compromised secret of a subgroup of said set of users.

10. (Cancelled)

11. (Original) The method of claim 1, wherein said compromised secret is shared by said plurality of users.

12. (Original) The method of claim 1, wherein said secrets enables secure communication.

13. (Previously Presented) In an environment that includes a plurality of users , wherein a first user possesses a set of keys, said set of keys including a first key that enables secure communication among a set of users, said set of users including at least said first user and a second user, a keying method, comprising:

(a) upon eviction of at least said second user, determining an updated first key using information that includes said first key and a second key, wherein said second key enables secure communication among a subgroup of said set of users, wherein said subgroup does not include users subject to said eviction;

wherein said determining uses a function having the following properties: (1) knowledge of said updated first key does not give knowledge of said first key or said second key, (2) knowledge of said first key does not give any knowledge of said updated first key, and (3) knowledge of said first key and said updated first key does not give any knowledge of said second key.

14. (Original) The method of claim 13, wherein only said second user is evicted.

15. (Original) The method of claim 13, wherein said second user and one or more other users in said set of users are evicted.

16. (Cancelled)

17. (Previously Presented) The method of claim 13, wherein said determining uses a one-way function.

18. (Original) The method of claim 17, wherein said updated first key is equal to F(first key, second key), wherein F() is a one-way function.

19. (Original) The method of claim 13, wherein said determining uses only said first key and said second key.

20. (Original) The method of claim 13, wherein said subgroup includes only said first user.

21. (Original) The method of claim 13, wherein said subgroup includes a plurality of users.

22.-27. (Cancelled)

28. (Previously Presented) A keying method in an environment having a plurality of users , each user being capable of storing a set of keys that enable secure communication among sets of said plurality of users, comprising:

(a) distributing first information that enables users to update, after eviction of one or more users, a set of compromised keys that are known to said one or more users without receiving new key information;

wherein said update does not include new secret information.

29. (Original) The method of claim 28, wherein said first information includes information that enables identification of a one-way function.

30. (Original) The method of claim 28, wherein said first information includes information that enables identification of said evicted one or more users.

31.-37. (Cancelled)

38. (Previously Presented) A secret sharing system, comprising.

a key server that distributes secret information to a plurality of users, wherein each user is sent secrets that are shared by respective sets of said plurality of users, said key server being operative to update at least one compromised secret known by at least one evicted user using at least one non-compromised secret that is not known by said at least one evicted user;

wherein said update does not include new secret information.

39. (Previously Presented) A computer program product, comprising:

computer-readable program code for causing a computer, in an environment that includes a plurality of users, wherein each user possesses secrets that are shared by respective sets of said plurality of users, to update at least one compromised secret known by at least one evicted user using at least one non-compromised secret that is not known by said at least one evicted user; and

a computer-usable medium configured to store the computer-readable program codes;

wherein said update does not include new secret information.

40. (Previously Presented) The method of claim 1, wherein said non-compromised secret utilized for said updating is known by all users in said plurality of users and is not known by said at least one evicted user.

41. (Previously Presented) The method of claim 40, wherein a single non-compromised secret is utilized to update a plurality of compromised secrets by using a one-way function with inputs of said single non-compromised secret and said non-compromised secret.

IX EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

N/A

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P089/00.175.01).

Respectfully submitted,

By: /KEVINZILKA/ Date: January 22, 2006

Kevin J. Zilka

Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660